42390.P8382X PATENT

UNITED STATES PATENT APPLICATION

for

METHOD AND APPARATUS FOR AUTHENTICATING AN HIERARCHY OF VIDEO RECEIVING DEVICES

Inventor(s):
Robert W. Faber
Brendan S. Traw
Gary L. Graunke
David A. Lee

prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, 7th Floor
Los Angeles, California 90025
(408)720-8300

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL 627465260US
Date of Deposit: September 29, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Claire Wallters
(Typed or printed name of person mailing paper or fee)
Claire Wallters
(Signature of person mailing paper or fee)
September 29, 2000
(Date signed)

Method And Apparatus For Authenticating An Hierarchy of Video Receiving Devices

Related Application

This application is a continuation-in-part application to U.S. Patent Applications number 09/385,590 and 09/385,592, both entitled Digital Video Content Transmission Ciphering and Deciphering Method and Apparatus, filed on August 29, 1999.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of content protection. More specifically, the present invention addresses authentication of hierarchically organized video receiving devices.

2. Background Information

In general, entertainment, education, art, and so forth (hereinafter collectively referred to as "content") packaged in digital form offer higher audio and video quality than their analog counterparts. However, content producers, especially those in the entertainment industry, are still reluctant in totally embracing the digital form. The primary reason being digital contents are particularly vulnerable to pirating. As unlike the analog form, where some amount of quality degradation generally occurs with each copying, a pirated copy of digital content is virtually as good as the "gold master". As a result, much effort have been spent by the industry in developing and adopting techniques to provide protection to the distribution and rendering of digital content.

Historically, the communication interface between a video source device (such as a personal computer) and a video sink device (such as a monitor) is an analog interface. Thus, very little focus has been given to providing protection for the transmission between the

source and sink devices. With advances in integrated circuit and other related technologies, a new type of digital interface between video source and sink devices is emerging. The availability of this type of new digital interface presents yet another new challenge to protecting digital video content. While in general, there is a large body of cipher technology known, the operating characteristics such as the volume of the data, its streaming nature, the bit rate and so forth, as well as the location of intelligence, typically in the source device and not the sink device, present a unique set of challenges, requiring a new and novel solution. Parent applications number 09/385,590 and 09/385,592 disclosed various protocol and cipher/deciphering techniques to authenticate a video sink device and protect transmission to the video sink device.

As technology advances, it is desired to be able to securely transmit digital video from a video source device to multiple hierarchically organized video sink devices. Thus, a need exist to authenticate devices and protect transmission in such hierarchical environment.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an example hierarchy of video source, repeater and sink devices incorporated with the teachings of the present invention, in accordance with one embodiment;

Figure 2 illustrates an overview of the authentication method of the present invention, in accordance with one embodiment;

Figure 3a illustrates the process for authenticating a video repeater device to a video source device, in accordance with one embodiment (which in one embodiment, is also the same process for authenticating a downstream video repeater device to an upstream video repeater device, a video sink device to a video repeater device, as well as a video sink device to a video source device);

Figure 3b illustrates the process for a video repeater device authenticating downstream video sink devices to an upstream video repeater device or a video source device; and

Figures 4a-4c illustrate a one way function suitable for use to practice the symmetric ciphering/deciphering process employed in one embodiment of the processes illustrated in **Fig. 3a-3b** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating an example hierarchy of video source, repeater and sink devices incorporated with the teachings of the present invention for authenticating the downstream video sink devices to the video source device is shown. As illustrated, example hierarchy **100** includes video source device **102**, video sink devices **104a-104d**, and video repeater devices **106a-106b**, coupled to each other as shown. As will be described in more detail below, each video device **102**, **104a-104d** or **106a-106b** includes an authentication unit (not shown) correspondingly incorporated with the applicable aspects of the teachings of present invention for authenticating video sink devices **104a-104d** to video source device **102**, to assure video source device **102** that post authentication video transmitted by video source device **102** will not be compromised by the downstream devices, such as making unauthorized copy of the video.

Except for the teachings of the present invention correspondingly incorporated therein, video source, repeater and sink devices **102**, **104a-104d**, and **106a-106b** are intended

to represent a broad range of digital devices known in the art. For examples, video source **102** may be any one of a number of digital "computing" devices known in the art, including but are not limited to, server computers, desktop computers, laptop computers, set-top boxes, DVD players and the like, and video sink devices **104a-104d** may be, but are not limited to, display devices such as Cathode Ray Tubes (CRT), flat panel displays, television sets, and the like, attached to these digital "computing" devices. Alternatively, one or more video sink devices **104-104d** may be another digital computing device with storage capability or a digital recording device. Video repeater devices **106a-106b** may be, but are not limited to, signal repeater devices.

These devices may be coupled to one another using any one of a number of communication links known in the art. Each of inter-device communication links for conducting the authentication process may or may not be the same communication link for transmitting the post-authentication video signals. In one embodiment, the devices are communicatively coupled to each other using serial communication links known in the art. Communications may be conducted with any pre-established protocols, which are of no particular relevance to the present invention.

Before proceeding to describing the authentication process of the present invention, it should be noted that while for ease of understanding, example hierarchy **100** includes only two repeater devices and four sink devices hierarchically organized into four hierarchy levels, video source device **102**, video sink device **104a** and video repeater device **106a**, video sink devices **104b-104c** and video repeater device **106b**, and video sink device **104d**, from the description to follow, it will be readily apparent to those skilled in the art, that the present invention may be practiced with any number of video repeater and sink devices hierarchically organized in two or more hierarchy levels. Any number of video repeater and sink devices may be present at each level. Further, a video repeater device may also be a video sink device. Nevertheless, for ease of understanding, the remaining description will treat repeater and sink devices as separate devices.

Figure 2 illustrates an overview of the authentication process of the present invention, in accordance with one embodiment. As shown, upon start up, such as power on or reset, at **202**, a downstream video repeater/sink device will first authenticate itself to the immediately upstream video source/repeater device. For example, in the case of example hierarchy **100** of **Fig. 1**, video sink device **104a** and video repeater device **106a** will authenticate itself to video source device **102**, video repeater device **106b** and video sink devices **104b-104c** will authenticate itself to video repeater device **106a**, and video sink device **104d** will authenticate itself to video repeater device **106b**.

For the illustrated embodiment, these authentications are all advantageously conducted with the same authentication process. That is, the operations performed by a pair of video source and sink devices, a pair of video source and repeater devices, a pair of video repeater devices, and a pair of video repeater and sink devices to authenticate the repeater/sink device to the source/repeater device, as the case may be, are basically the same operations. To differentiate an authenticating video repeater device, such as **106a** or **106b**, from a video sink device, such as **104a**, **104b**, or **104c**, a video repeater device, such as **106a** or **106b**, will identify itself to the immediately upstream device, such as device **102a** or **106a**, that the device is a repeater device, and a video sink device, such a **104a-104d** would not make such identification, thereby facilitating the participate devices to know whether the remaining authentication process, to authenticate the downstream video sink devices need to be performed or not.

At **204**, an upstream device, such as source device **102** or repeater device **106a**, will await the downstream device who has identified itself as a repeater device, such as device **106a** and **106b**, to provide the authentication information of all their downstream video sink devices, in the case of repeater device **106a**, sink devices **104b-104c**, and the case of repeater device **106b**, sink devices **104c**. When ready, that is having aggregated all authentication information of the downstream sink devices, repeater device **106a/106b** would perform the

remaining operations authenticating all downstream video sink devices to its immediately upstream device. As examples, in the case of example hierarchy **100** of **Fig. 1**, upon authenticating video sink device **104d**, video repeater device **106b** would authenticate video sink device **104d** to immediately upstream video repeater device **106a**, and for video repeater device **106a**, upon first authenticating video repeater device **106b** and video sink devices **104b-104c**, and then authenticating video sink device **104d**, video repeater device **106a** would authenticate video sink devices **104b-104d** to video source device **102**. In each case, i.e. video repeater device **106b** authenticating video sink device **104d** to video repeater device **106a**, and video repeater device **106a** authenticating video sink devices **104b-104d** to video source device **102**, video repeater device **106a/106b** also provides the topology information of the sink devices to video repeater/source device **106a/102**. In other words, video repeater device **106b** will inform video repeater device **106a** that video sink device **104d** is immediately downstream from it, whereas video repeater device **106a** will inform video source device **102** that video sink devices **104b-104c** are immediately downstream from it, and video sink device **104d** is downstream from it via video repeater device **106b**.

Accordingly, it can be seen, except for practical or commercial reasons, the present invention has no structural limit to the number video sink devices that can be attached to a video repeater device at each hierarchy level, nor is there any structural limit on to the number of hierarchy levels.

In one embodiment, the identical authentication process employed by the devices to authenticate itself to the immediately upstream device, as well as the authentication process employed by a repeater device to authenticate all downstream video sink devices to an immediately upstream video source/repeater device is a cooperative process that involves a symmetric ciphering/deciphering process independently performed by the authentication parties.

Figures 3a-3b illustrate two overviews of the symmetric ciphering/deciphering process based method for authenticating a downstream device to an immediately upstream device, and for a repeater device to authenticate all its downstream sink devices to its immediately upstream device, in accordance with one embodiment. For the illustrated embodiment, all devices correspondingly incorporated with the applicable portions of the teachings of the present invention, video source device **102**, sink devices **104a-104b** and repeater devices **106a-106d**, are assumed to be equipped with an array of "cryptographic" device keys (Akey or Bkey) by a certification authority (hereinafter, simply device keys). In one embodiment, the assignment of these "cryptographic" device keys are performed in accordance with the teachings of the co-pending U.S. Patent Application number 09/275,722, filed on March 24, 1999, entitled Method and Apparatus for the Generation of Cryptographic Keys, having common assignee with the present application.

As illustrated in **Fig. 3a**, the authentication unit of an immediately upstream device, e.g. video source device **102**, video repeater device **106a** or video repeater device **106b**, kicks off the authentication process with each immediately downstream device by generating a basis value (A_n) to the symmetric ciphering/deciphering process, and providing the basis value along with a device key selection vector (A_n, Ak_{sv}) to the immediate downstream device, e.g. video sink device **104a**/video repeater devices **106a**, video repeater device **106b**/video sink devices **104b-104c**, and video sink device **104c**. [Further details on the assignment of device key selection vectors to devices may also be found in the aforementioned application number 09/275,722.] For the example hierarchy **100** of **Fig. 1**, video source device **102** will kick off two authentication processes, one with video sink device **104a** and another one with video repeater device **106a**, video repeater device **106a** will kick off three authentication processes, one with video repeater device **106b** and two others, on each, with video sink device **106b**, and video repeater device **106b** will kick off an authentication process with video sink device **104d**. For the illustrated embodiment, basis

value A_n is a pseudo random number. A_n may be generated in any one of a number of techniques known in the art.

In response, for each of the authentication processes, the authentication unit of the immediately downstream device, e.g. video sink device **104a**/video repeater device **106a**, video repeat device **106b**/video sink devices **104b**/**104c**, and video sink device **104d** responds by providing its device key selection vector (Bk_{sv}) and an indicator (Repeater) indicating whether the downstream device is a repeater device or not. In one embodiment, the Repeater indicator is a 1-bit indicator set to "1" if the downstream device is a repeater device, and set to "0" if the downstream device is not a repeater device.

Thereafter, for each of the authentication processes, each of the authentication units, of the upstream and downstream devices, will independently generate a verification value R_0 and R_0', using the basis value A_n, their deviec keys, and the exchanged device key selection vectors AK_{sv} and BK_{sv} and the Repeater indicator. The authentication unit of the downstream device will provide its independently generated verification value R_0' to the upstream device, and the authentication unit of the upstream device in turn compares the two verification values, and depending on whether the two verification values successfully compares, uses the provided Bk_{sv} to determine if the downstream device is an authorized device or a device to be trusted. The upstream device accepts Bk_{sv} and uses it to compare against an authorization list to determine whether the downstream device is an authorized or trustworthy device if R_0 equals R_0', otherwise, if R_0 not equals R_0', the downstream device is deemed to be an unauthorized or untrustworthy device. In one embodiment, subsequent video transmissions, if any, would not be passed by the upstream device to the immediately downstream device that failed the authentication process.

For the illustrated embodiment, the authentication unit of the upstream/downstream device independently generates the verification value R_0/R_0' by first generating an authentication key K_m/K_m'. As illustrated, authentication key K_m/K_m' is generated by summing device key Akey/Bkey over device key selection vector BK_{sv}/AK_{sv} (see application

number 09/275,722 for detail). Next, the authentication unit of the upstream/downstream device independently generates the verification value R_0/R_0' using K_m/K_m', Repeater indicator, and A_n). In one embodiment, the authentication unit generates R_0/R_0' employing a "one way function" with K_m/K_m' and Repeater indicator concatenated with A_n.

For the illustrated embodiment, each authentication unit also generates, as part of the process for generating R_0/R_0', a shared secret M_0/M_0' and a session key K_s/K_s'. Shared secret M_0/M_0' is used in the subsequent authentication of the video sink devices downstream to a video repeater device, as well as the protection of the video transmitted posted authentication. Session key K_s/K_s' is used in the protection of the video transmitted posted authentication. Employment of M_0/M_0' and K_s/K_s' to protect the video transmitted post authentication is the subject matters of the parent applications. See the respective applications for details.

At this point, the authentication process is completed between a video source device and a video sink device, and between a video repeater device and a video sink device. For video source device and video repeater device, and for video repeater device and video repeater device, the process continues as illustrated in **Fig. 3b** for the immediately downstream video repeater device to authenticate to the immediately upstream video source/repeater device all downstream video sink devices.

As illustrated, for each upstream device, where the immediately downstream device has identified itself as a repeater device, it awaits for a "Ready" signal from the immediately downstream repeater device, denoting the downstream repeater device has reliably obtained the device key selection vectors of the downstream video sink devices and the downstream repeater device is ready to provide the list of device key selection vectors to the upstream device for authentication. This operation advantageously allows the device key selection vectors of the downstream video sink devices to be successively "percolated" upward through the downstream repeater devices.

Upon having reliably received all the device key selection vectors of the downstream video sink devices (Bk_{sv} list), the downstream repeater device provides the reliably

accumulated Bk_{sv} list to its immediate upstream repeater/source device. For examples, for example hierarchy **100** of **Fig. 1**, video repeater device **106b**, upon reliably obtaining Bk_{sv} of video sink device **104d**, provides the particular Bk_{sv} to video repeater device **106a**. For video repeater device **106a**, upon authenticating Bk_{sv} of video sink devices **104b-104c** and upon reliably provided Bk_{sv} of video sink device **104d** by video repeater device **106b**, it provides Bk_{sv} of all downstream video sink devices, **104d** as well as **104b** and **104c** to video source device **102**.

For the illustrated embodiment, each of the downstream repeater device provides the Bk_{sv} list along with a verification signature (V') and the topology information of the downstream video sink devices. For example, the topological information provided by video repeater device **106a** to video source device **102** denotes to video source device **102** of the fact that video sink device **104d** is actually downstream to video repeater device **106a** through video repeater device **106b**, however, video sink devices **104b-104c** are immediately downstream to video repeater device **106a**.

For the illustrated embodiment, each authentication unit of an immediately downstream video repeater device generates the verification signature V' using a predetermined hash function hashing the Bk_{sv} list, the topology "vector", and the earlier described shared secret M_0'. In one embodiment, the Bk_{sv} list, the topology "vector", and the earlier described shared secret M_0' are concatenated together. The predetermined hash function may be any "secure" hashing function known in the art.

Upon receiving the Bk_{sv} list, the verification signature, and the topology "vector", in like manner, the immediately upstream source/repeater device independently generates its own verification value V. In one embodiment, the immediately upstream source/repeater device independently generates its own verification value V, using the same hash function, the provided Bk_{sv} list, the topology "vector", and its own independently generated shared secret M_0. Upon generating its own verification value V, the immediately upstream source/repeater device compares the two verification values V and V' to determine whether

to accept the provided Bk_{sv} list. In one embodiment, the immediately upstream source/repeater device accepts the provided Bk_{sv} list (when V=V') and compares the list against an authentication list to determine whether the video sink devices are authorized or trustworthy devices, and rejects the provided Bk_{sv} list if V does not equal V'. If the Bk_{sv} list is rejected, the video sink devices are deemed to be unauthorized or untrustworthy sink devices. When that occurs, future video will not be provided to the immediately downstream video repeater device, thereby protecting the video from being sent to the unauthorized or untrustworthy video sink devices.

Figures 4a-4c illustrate a one-way function suitable for use to practice the symmetric ciphering/deciphering process of **Fig. 3a-3b**, in accordance with one embodiment. As alluded to earlier, in one embodiment, this one-way function is a part of the authentication unit of each of the video source/repeater/sink devices. As illustrated in **Fig. 4a**, the one way function **800** includes a number of linear feedback shift registers (LFSRs) **802** and combiner function **804**, coupled to each other as shown. LFSRs **802** and combiner function **804** are collectively initialized with the appropriate keys and data values. During operation, the values are successively shifted through LFSRs **802**. Selective outputs are taken from LFSRs **802**, and combiner function **804** is used to combine the selective outputs to generate the desired outputs.

In one embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follow:

LFSR	Polynomial	Combining Function Taps		
		0	1	2
3	$X^{17}+x^{15}+x^{11}+x^{5}+1$	5	11	16
2	$X^{16}+x^{15}+x^{12}+x^{8}+x^{7}+x^{5}+1$	5	9	15
1	$X^{14}+x^{11}+x^{10}+x^{7}+x^{6}+x^{4}+1$	4	8	13
0	$X^{13}+x^{11}+x^{9}+x^{5}+1$	3	7	12

The initialization of the LFSRs and the combiner function, more spefically, the shuffling network of the combiner function, is in accordance with the following table.

	Bit Field		Initial Value
LFSR3	[16]		Complement of input bit 47
	[15:0]		Input bits[55:40]
LFSR2	[15]		Complement of input bit 32
	[14:0]		Input bits[39:25]
LFSR1	[13]		Complement of input bit 18
	[12:0]		Input bits[24:12]
LFSR0	[12]		Complement of input bit 6
	[11:0]		Input bits[11:0]
Shuffle Network	Register A Register B		0 1

The combined result is generated from the third set of LFSR outputs, using the first and second set of LFSR outputs as data and control inputs respectively to combiner function **804**. The third set of LFSR outputs are combined into a single bit.

Fig. 4b illustrates combiner function **804** in further detail, in accordance with one embodiment. As illustrated, combiner function **804** includes shuffle network **806** and XOR **808a-808b**, serially coupled to each other and LFSRs **802** as shown. For the illustrated embodiment, shuffle network **806** includes four binary shuffle units **810a-810d** serially coupled to each other, with first and last binary shuffle units **810a** and **810d** coupled to XOR **808a** and **808b** respectively. XOR **808a** takes the first group of LFSR outputs and combined them as a single bit input for shuffle network **806**. Binary shuffle units **810a-810d** serially propagate and shuffle the output of XOR **808a**. The second group of LFSR outputs are used to control the shuffling at corresponding ones of binary shuffle units **810a-810d**. XOR **808b** combines the third set of LFSR outputs with the output of last binary shuffle unit **810d**.

Fig. 4c illustrates one binary shuffle unit **810*** (where * is one of **a-d**) in further detail, in accordance with one embodiment. Each binary shuffle unit **810*** includes two flip-flops **812a** and **812b**, and a number of selectors **814a-814c**, coupled to each other as shown. Flip-flops **812a** and **812b** are used to store two state values (A, B). Each selector **814a, 814b** or **814c** receives a corresponding one of the second group of LFSR outputs as its control signal. Selector **814a-814b** also each receives the output of XOR **808a** or an immediately preceding binary shuffle unit **810*** as input. Selector **814a-814b** are coupled to flip-flops **812a-812b** to output one of the two stored state values and to shuffle as well as modify the stored values in accordance with the state of the select signal. More specifically, for the illustrated embodiment, if the stored state values are (A, B), and the input and select values are (D, S), binary shuffle unit **810*** outputs A, and stores (B, D) if the value of S is "0". Binary shuffle unit **810*** outputs B, and stores (D, A) if the value of S is "1".

Accordingly, a novel method and apparatus for authenticating hierarchically organized video repeater and sink devices has been described.

Epilogue

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. Thus, the present invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and scope of the appended claims.